



WLR-2002

Wireless Mobile Router 300N



User Manual

Revision: 1.0

TABLE OF CONTENTS

1	KEY FEATURES.....	4
2	PACKAGE CONTENTS	5
3	PRODUCT LAYOUT	6
4	NETWORK + SYSTEM REQUIREMENTS	8
5	WLR-2002 PLACEMENT.....	8
6	SETUP LAN, WAN.....	9
7	PC NETWORK ADAPTER SETUP	10
8	BRINGING UP THE WLR-2002.....	14
9	INITIAL SETUP OF THE WLR-2002	14
10	CONFIGURATION WIZARD	23
11	WIRELESS SETTINGS.....	25
12	FIREWALL SETTINGS.....	35
13	ADVANCED SETTINGS.....	41
14	TOOLBOX SETTINGS	51

Introduction

Congratulations on your purchase of the WLR-2002 Wireless Mobile Router 300N. The WLR-2002 is compliant with 802.11n and up to 6 times faster than standard 802.11g based routers while still being compatible with 802.11g & 802.11b devices.

At 300 Mbps wireless transmission rate, the Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel, giving you seamless access to multimedia content. Robust RF signal travels farther, eliminating dead spots and extending the network range. For data protection and privacy, the WLR-2002 encodes all wireless transmissions with WEP, WPA or WPA2 encryption.

With the built-in DHCP Server & powerful SPI firewall, the WLR-2002 protects your computers against intruders and most known Internet attacks but provides safe VPN pass-through. With the small form factor and built-in power supply, the WLR-2002 is ideal for use on the move, in hotels or on campsites.

Besides, it also provides a USB port which let you easily share a 3G/UMTS modem.

1 Key Features

Features	Advantages
Incredible Data Rate up to 300Mbps*	Heavy data payloads such as MPEG video streaming
IEEE 802.11n compliant and backward compatible with 802.11b/g	Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices with legacy protection
USB port for 3G USB modem	Wireless internet everywhere, even without broadband availability.
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	Avoids the attacks of Hackers or Viruses from Internet
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	Provide mutual authentication (Client and dynamic encryption keys to enhance security
OPS (One Push Setup)	Connect a client via a secure connection with one push of a button.

** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*


2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. WLR-2002 Router
2. Power Cable
3. Quick Install Guide
4. CD (User's Manual)
5. Warranty card
6. UTP cable

3 Product Layout



Port	Description
AC 100v~240v	Connect the AC power cable to this port
RJ45	Connect your ADSL/Cable modem to this port
3G 	Connect your 3G USB modem to this port

Top Cover

On the top cover you can see the LEDs that show the functionality of the device. Also present is the OPS button which allows you to connect your computer with a secure wireless connection with the push of a button.



From left to right the LED's show the following:

Power, Ethernet, WPS, WLAN, 3G (USB)

Button	Description
OPS	Press 2 seconds for OPS mode
	Press 10 seconds to reset the router
	Press 15 Seconds to reset the router to factory defaults.

Back label

The back label describes the IP address, login details, SSID, security and code.



4 Network + System Requirements

To begin using the WLR-2002, make sure you meet the following as minimum requirements:

- PC/Notebook.
- Operating System – Microsoft Windows XP/2000/VISTA
- Wi-Fi card/USB client (802.11 b/g/n).
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45), or a 3G USB modem.
- Web-Browser (Internet Explorer, Safari, Firefox, Opera)

5 WLR-2002 Placement

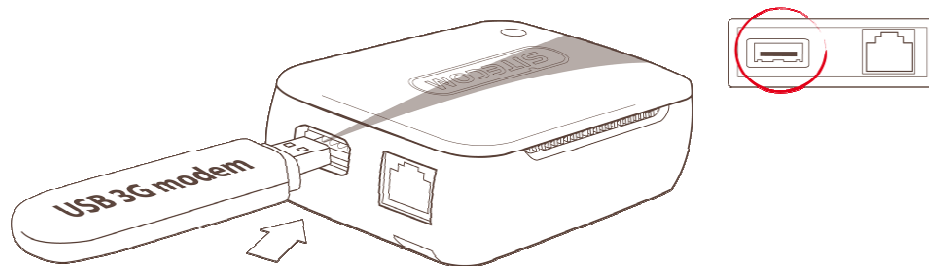
You can place the WLR-2002 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Mobile Router 300N in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem in case you're using the WAN port.

6 Setup LAN, WAN

The WLR-2002 has one Ethernet port that doubles as a WAN (Internet) port and a LAN port.

When no 3G USB client is inserted in the USB port, the port functions as WAN.
When a 3G USB client is inserted in the USB port, the port functions as LAN.

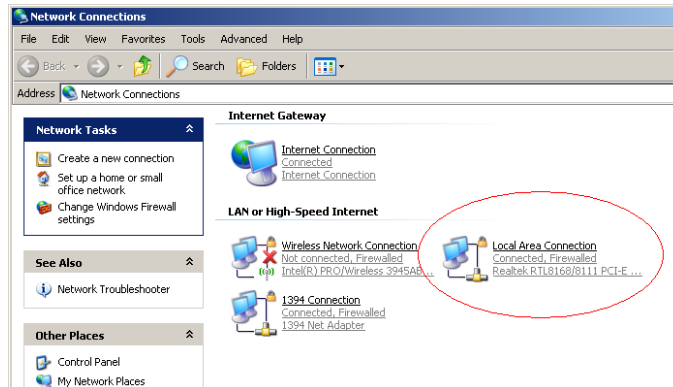
To use only the 3G USB connection, just insert a 3G USB client into the designated USB port.



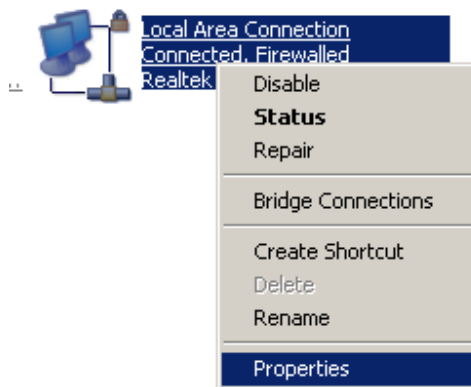
7 PC Network Adapter setup

Windows XP

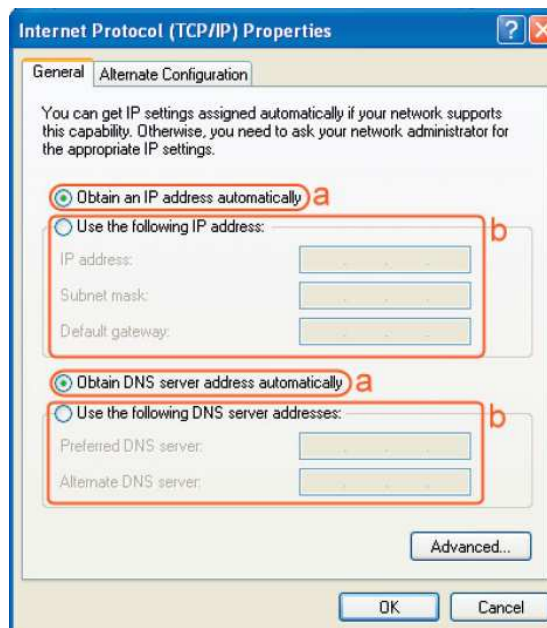
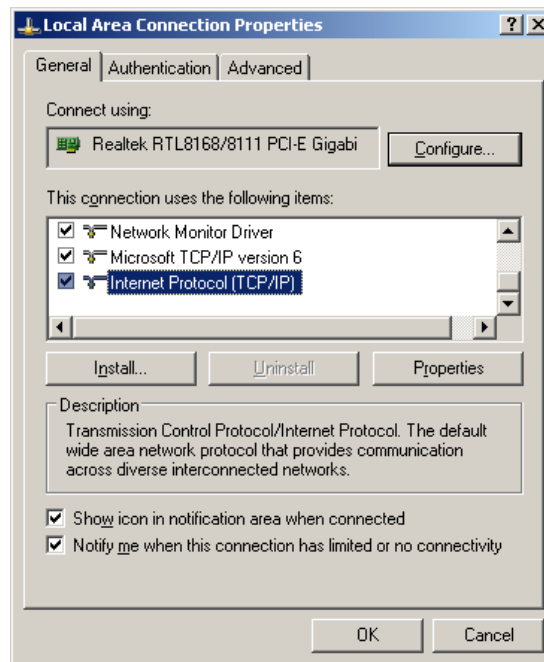
- Enter [Start Menu] → select [Control panel] → select [Network].



- Select [Local Area Connection]) icon=>select [properties]



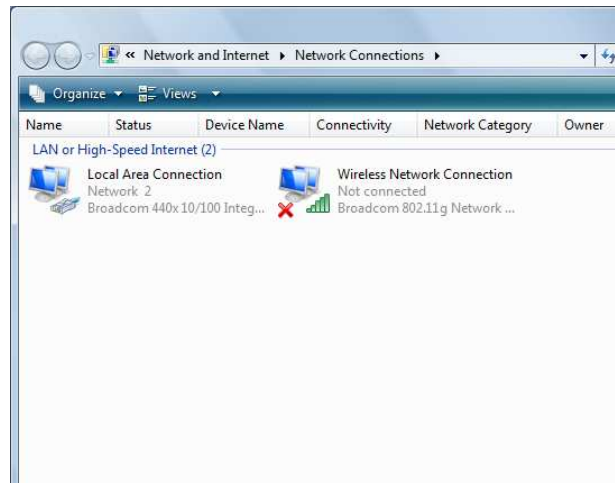
- Select [Internet Protocol (TCP/IP)] =>Click [Properties].



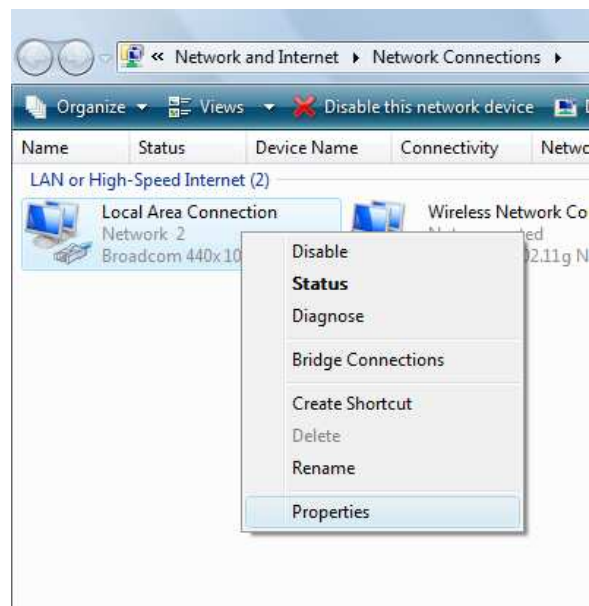
- Select the [General] tab.
The WLR-2002 supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

Windows Vista

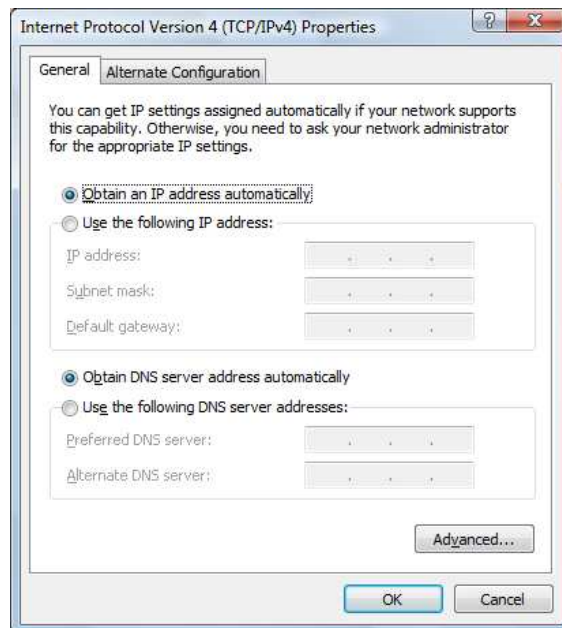
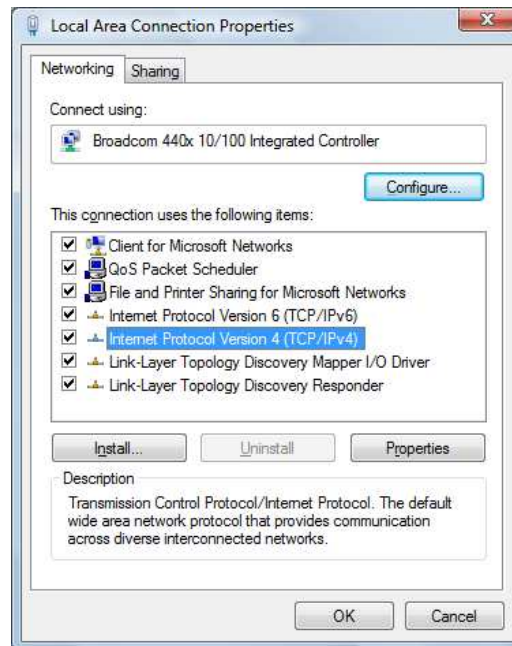
- Enter [Start Menu] → select [Control panel] → select [View network status and tasks] -> select [Manage network connections].



- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol Version 4 (TCP/IPv4)] =>Click [Properties].



- Select the [General] tab.

The WLR-2002 supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

8 Bringing up the WLR-2002

Connect the supplied power-adaptor to the power inlet port and connect it to a wall outlet. The WLR-2002 automatically enters the self-test phase. During self-test phase, the Power LED will be lit continuously to indicate that this product is in normal operation.

9 Initial Setup of the WLR-2002

LOGIN procedure

1. OPEN your browser (e.g. Internet Explorer).



2. Type <http://192.168.0.1> in the address bar and press [Enter].



3. Type user name and password (default is admin/admin).



A Windows-style dialog box titled "Connect to 192.168.0.1". It features a blue header bar with a key icon. The main text area contains a warning: "The server 192.168.0.1 requires a username and password. Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection)." Below this, there are input fields for "User name:" (containing "admin") and "Password:" (masked with dots). A checkbox labeled "Remember my password" is checked. At the bottom are "OK" and "Cancel" buttons.

4. Click **OK**.
5. You will see the home page of the WLR-2002.



The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The header includes the product name "wireless mobile router 300N" and the Sitecom logo. A navigation bar contains tabs: Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A "Choose your language" dropdown is on the right. Below the navigation bar, the "System Status" tab is selected. A descriptive paragraph explains the status page's function. A "System" section displays a table of router information.

System	
Model :	Wireless Travel Router
Uptime :	19 sec
Hardware Version :	Rev. A
Serial Number :	000000064
Boot Code Version :	1.0
Runtime Code Version :	1.0

The System status section allows you to monitor the current status of your router: the UP time, hardware information, serial number as well as firmware version information is displayed here.

LAN settings

The LAN tab gives you the opportunity to change the IP settings of the WLR-2002.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings Firewall Advanced Settings Toolbox Choose your language ▼

System Status **DHCP Server** Device Status Internet Status DHCP Status Log Statistics

You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

LAN IP

IP Address : 192.168.0.1

IP Subnet Mask : 255.255.255.0

802.1d Spanning Tree : Disabled ▼

DHCP Server : Enabled ▼

Lease Time : Forever ▼

DHCP Server

Start IP : 192.168.0.100

End IP : 192.168.0.200

Domain Name : sitecomwlr2002

Apply Cancel

Click **<Apply>** at the bottom of this screen to save any changes.

IP address 192.168.0.1. It is the router's LAN IP address (Your LAN clients default gateway IP address).

IP Subnet Mask 255.255.255.0 Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree is Disabled by default. If the 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server Enabled by default. You can enable or disable the DHCP server. When DHCP is disabled no IP-addresses are assigned to clients and you have to use static IP-addresses. When DHCP server is enabled your computers will be assigned an IP-address automatically until the lease time expires.

Lease Time Forever. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.

IP Address Pool You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.

Note: *default IP range 192.168.0.100 - 192.168.0.200. If you want your PC(s) to have a static/fixed IP address, then you'll have to choose an IP address outside this IP address Pool*

Domain Name You can specify a Domain Name for your LAN, or just keep the default (sitecomwlr2002).

Device Status

View the Broadband router's current configuration settings. Device Status displays the configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section.

The screenshot shows the web interface of a Sitecom 300N wireless mobile router. The page title is "wireless mobile router 300N" with the Sitecom logo. The navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is set to "Choose your language". Below the navigation bar, a sub-menu highlights "Device Status" among other options like System Status, DHCP Server, Internet Status, DHCP Status, Log, and Statistics.

View the current setting status of this device.

Mode :	AP
Channel :	1

SSID_1

ESSID :	Sitecom5FAB74
Security :	WPA2 pre-shared key
BSSID :	00:0C:F6:5F:AB:74
Associated Clients :	0

LAN Configuration

IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled
MAC Address :	00:0C:F6:5F:AB:74

Internet Status

This page displays whether the WAN port is connected to a Cable/DSL or 3G connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press **Renew** button to renew your WAN IP address.

The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The page is titled "Internet Status" and displays the current internet connection status and related information. The interface includes a navigation bar with tabs for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is also present. The main content area shows the following status information:

Attain IP Protocol :	Mobile 3G
3G USB Modem Status :	Ready
SIM Status :	SIM Card need PIN code
Signal :	No Signal
IP Address :	---
Subnet Mask :	---
Default Gateway :	---
Primary DNS :	---

At the bottom right, there are two buttons: "Connect" and "Disconnect".

DHCP Client Status

DHCP This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the Refresh button to update the available information.

You can check **Enable Static DHCP IP**. It is possible to add more static DHCP IP's. They are listed in the table **Current Static DHCP Table**. IP can be deleted at will from the table.

Click **apply** button to save the changed configuration.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings Firewall Advanced Settings Toolbox Choose your language

System Status DHCP Server Device Status Internet Status **DHCP Status** Log Statistics

This table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

IP address	MAC address	Expiration Time
192.168.0.196	00:1C:23:A5:B8:4C	Forever

Refresh

☐ Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Add Reset

Current Static DHCP Table:

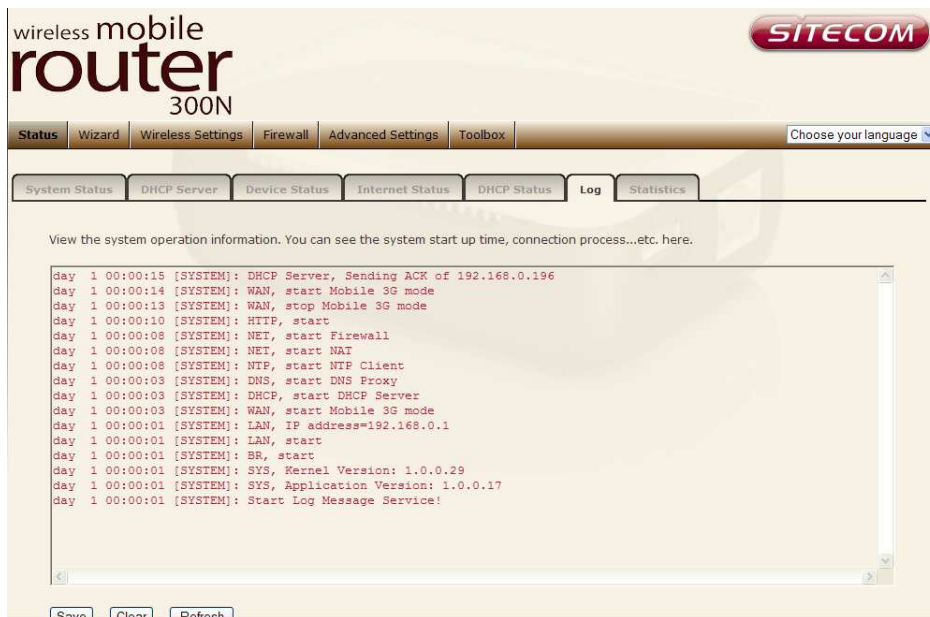
NO.	IP address	MAC address	Select
-----	------------	-------------	--------

Delete Selected Delete All Reset

Apply Cancel

WLR-2002 Log

View the operation **log of the WLR-2002**. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.



wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings Firewall Advanced Settings Toolbox Choose your language

System Status DHCP Server Device Status Internet Status DHCP Status **Log** Statistics

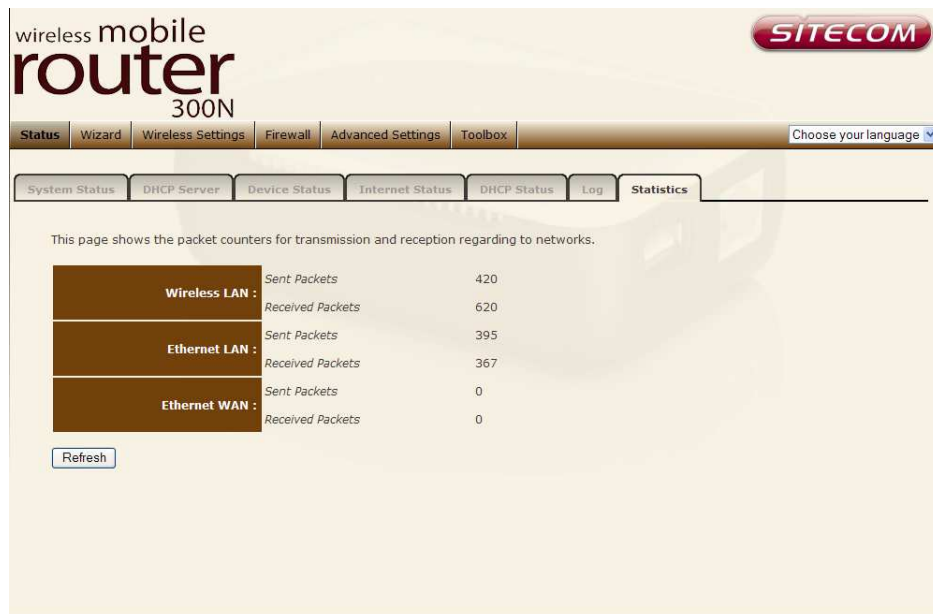
View the system operation information. You can see the system start up time, connection process...etc. here.

```
day 1 00:00:15 [SYSTEM]: DHCP Server, Sending ACK of 192.168.0.196
day 1 00:00:14 [SYSTEM]: WAN, start Mobile 3G mode
day 1 00:00:13 [SYSTEM]: WAN, stop Mobile 3G mode
day 1 00:00:10 [SYSTEM]: HTTP, start
day 1 00:00:08 [SYSTEM]: NET, start Firewall
day 1 00:00:08 [SYSTEM]: NET, start NAT
day 1 00:00:08 [SYSTEM]: NTP, start NTP Client
day 1 00:00:03 [SYSTEM]: DNS, start DNS Proxy
day 1 00:00:03 [SYSTEM]: DHCP, start DHCP Server
day 1 00:00:03 [SYSTEM]: WAN, start Mobile 3G mode
day 1 00:00:01 [SYSTEM]: LAN, IP address=192.168.0.1
day 1 00:00:01 [SYSTEM]: LAN, start
day 1 00:00:01 [SYSTEM]: BR, start
day 1 00:00:01 [SYSTEM]: SYS, Kernel Version: 1.0.0.29
day 1 00:00:01 [SYSTEM]: SYS, Application Version: 1.0.0.17
day 1 00:00:01 [SYSTEM]: Start Log Message Service!
```

Save Clear Refresh

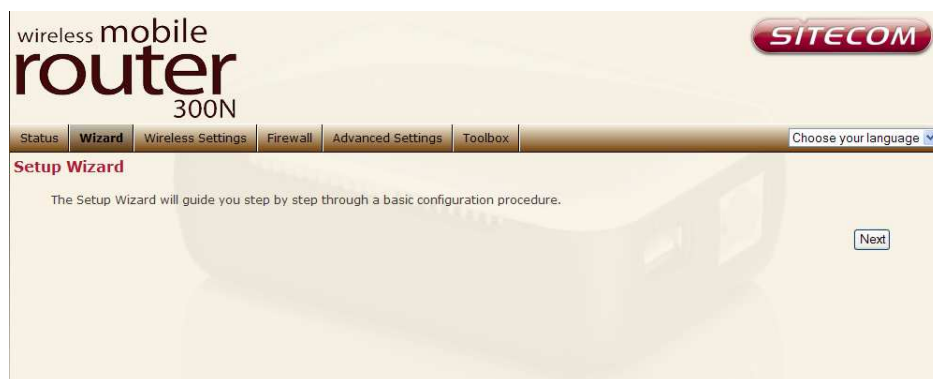
WLR-2002 Statistics

Shows the counters of packets sent and received on WAN, LAN & WLAN.



10 Configuration Wizard

Click **Wizard** to configure the router. The Setup wizard will now be displayed; check that the modem is connected and click **Next**.



Select your country from the Country list. Select your internet provider. Alternatively you can select "Mobile 3G" to set the WLR-2002 up for a 3G/UMTS connection. Click **Next**.



Depending on the chosen provider, you may need to enter your user name and password, MAC address or hostname in the following window. After you have entered the correct information, click **Next**.

wireless mobile
router
300N

SITECOM

StatusWizardWireless SettingsFirewallAdvanced SettingsToolbox

Choose your language

Please, enter the data which is supplied by your ISP.

Login Method :	PPP over Ethernet		
Username :	<input type="text"/>		
Password :	<input type="password"/>		
Service :	<input type="text"/>		
MTU :	<input type="text" value="1452"/>	(512<=MTU Value<=1492)	
Connection Type :	<input type="text" value="Keep connection"/>	<input type="button" value="Connect"/>	<input type="button" value="Disconnect"/>
Idle Time :	<input type="text" value="10"/>	(1-1000 Minutes)	

wireless mobile
router
300N

SITECOM

StatusWizardWireless SettingsFirewallAdvanced SettingsToolbox

Choose your language

Please, enter the data which is supplied by your ISP.

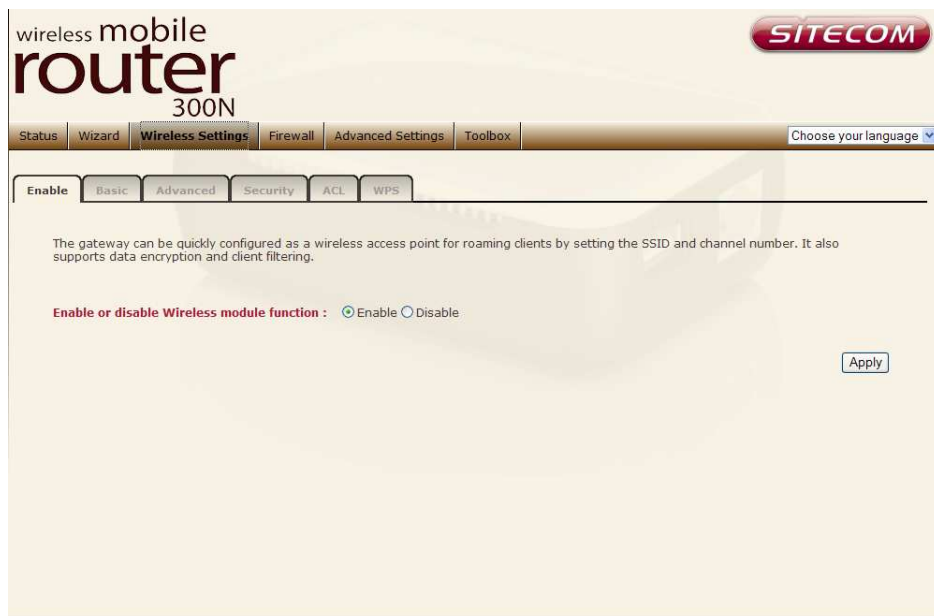
Login Method :	<input type="text" value="Mobile 3G"/>		
Pin Code:	<input type="text"/>		
APN Code:	<input type="text"/>		
Phone Number:	<input type="text"/>		
User Name:	<input type="text"/>		
Password:	<input type="password"/>		
Type:	<input type="text" value="Keep connection"/>	<input type="button" value="Connect"/>	<input type="button" value="Disconnect"/>
Idle Time :	<input type="text" value="10"/>	(1-1000 Minutes)	

Click **APPLY** to complete the configuration.

11 Wireless Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

Wireless Function



Enable or Disable Wireless function here. Click **Apply** and wait for module to be ready & loaded.

Basic Settings

The screenshot shows the configuration interface for a Sitecom 300N wireless mobile router. The page is titled "wireless mobile router 300N" and features the Sitecom logo. A navigation bar includes tabs for Status, Wizard, Wireless Settings (selected), Firewall, Advanced Settings, and Toolbox. A language selection dropdown is also present. Below the navigation bar, there are sub-tabs: Enable, Basic (selected), Advanced, Security, ACL, and WPS. The main content area explains that this page is for defining ESSID and Channel for the wireless connection. It contains five configuration fields: Mode (set to AP), Band (set to 2.4 GHz (B+G+N)), Enable SSID# (set to 1), SSID1 (set to Sitecom5FAB74), and Channel (set to 1). At the bottom right, there are Apply and Cancel buttons.

Field	Value
Mode :	AP
Band :	2.4 GHz (B+G+N)
Enable SSID# :	1
SSID1 :	Sitecom5FAB74
Channel :	1

- Mode** Allows you to set the AP to AP, Station, Bridge or WDS mode.
- Band** Allows you to set the AP fixed at 802.11b or 802.11g mode. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time.
- SSID** This is the name of the wireless signal which is broadcasted. All the devices in the same wireless LAN should have the same ESSID.
- Channel** The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Advanced Settings

This tab allows you to set the advanced wireless options. The options included are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.



The screenshot shows the 'Advanced Settings' tab for a Sitecom wireless mobile router 300N. The page has a navigation bar with tabs: Status, Wizard, Wireless Settings (selected), Firewall, Advanced Settings, and Toolbox. Below the navigation bar, there are sub-tabs: Enable, Basic, Advanced (selected), Security, ACL, and WPS. A warning message states: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.' The settings are as follows:

Setting	Value	Range
Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(1-2347)
Beacon Interval	100	(20-1024 ms)
DTIM Period	1	(1-255)
Data Rate	Auto	
N Data Rate	Auto	
Channel Bandwidth	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
Preamble Type	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power	100 %	

Buttons: Apply, Cancel

Fragment Threshold "Fragment Threshold" specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth is the range of frequencies that will be used.

Preamble Type The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

TX Power can be set to a bare minimum or maximum power.

Security

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.

Disable


When you choose to disable encryption, it is very insecure to operate the WLR-2002.



The screenshot shows a web interface for configuring wireless security. At the top, there are tabs: 'Enable', 'Basic', 'Advanced', 'Security' (selected), 'ACL', and 'WPS'. Below the tabs, a message states: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' The 'Encryption' dropdown menu is set to 'Disable'. Below this, there is a checkbox labeled 'Enable 802.1x Authentication' which is currently unchecked. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Enable 802.1x Auth

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication



The screenshot shows the same web interface as before, but now the 'Enable 802.1x Authentication' checkbox is checked. Below the checkbox, there are three input fields: 'RADIUS Server IP Address', 'RADIUS Server Port' (with the value '1812' entered), and 'RADIUS Server Password'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.



The screenshot shows a configuration interface for WEP encryption. It features a table with the following rows and columns:

Field	Value
Encryption :	WEP
Key Length :	64-bit
Key Type :	ASCII (5 characters)
Default Key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

Key Length You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Format You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Key1 - Key4 The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.



A screenshot of a web-based configuration form for WPA Pre-shared Key. The form has a light beige background with a subtle keyboard pattern. It contains four rows of configuration options, each with a label and a corresponding input field or control. The first row is 'Encryption' with a dropdown menu set to 'WPA pre-shared key'. The second row is 'WPA Type' with three radio buttons: 'WPA(TKIP)' (selected), 'WPA2(AES)', and 'WPA2 Mixed'. The third row is 'Pre-shared Key Type' with a dropdown menu set to 'Passphrase'. The fourth row is 'Pre-sharedKey' with a text input field. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Encryption :	WPA pre-shared key
WPA Type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key Type :	Passphrase
Pre-sharedKey :	

Apply Cancel

WPA-Radius

Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses **TKIP** or CCMP (**AES**) to change the encryption key frequently. Press **Apply** button when you are done.



A screenshot of a web-based configuration form for WPA-RADIUS. The form has a light beige background with a subtle keyboard pattern. It contains five rows of configuration options, each with a label and a corresponding input field or control. The first row is 'Encryption' with a dropdown menu set to 'WPA RADIUS'. The second row is 'WPA Type' with three radio buttons: 'WPA(TKIP)' (selected), 'WPA2(AES)', and 'WPA2 Mixed'. The third row is 'RADIUS Server IP Address' with a text input field. The fourth row is 'RADIUS Server Port' with a text input field containing '1812'. The fifth row is 'RADIUS Server Password' with a text input field. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Encryption :	WPA RADIUS
WPA Type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP Address :	
RADIUS Server Port :	1812
RADIUS Server Password :	

Apply Cancel

ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

wireless mobile
router
300N

SITECOM

Status Wizard **Wireless Settings** Firewall Advanced Settings Toolbox Choose your language ▼

Enable Basic Advanced Security **ACL** WPS

For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point.

MAC Address Filtering Table

NO.	MAC address	Comment	Select
-----	-------------	---------	--------

Delete Selected Delete All Reset

☐ **Enable Wireless Access Control**

New : MAC address : Comment : Add Reset

Apply Cancel

Enable wireless access control Enables the wireless access control function

Adding an address into the list Enter the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

Remove an address from the list If you want to remove a MAC address from the "Current Access Control List ", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPS

Wi-Fi Protected Setup (WPS) is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

The screenshot displays the web configuration interface for a Sitecom 300N wireless mobile router. The page title is "wireless mobile router 300N" with the Sitecom logo in the top right corner. A navigation bar includes links for Status, Wizard, Wireless Settings (selected), Firewall, Advanced Settings, and Toolbox. A language selection dropdown is also present. Below the navigation bar, a tabbed interface shows "Enable", "Basic", "Advanced", "Security", "ACL", and "WPS" (selected). The WPS section features a "WPS : ☒ Enable" toggle. Under the heading "Wi-Fi Protected Setup Information", the following details are listed: "WPS Current Status : Configured", "Self Pin Code : 62698122", "SSID : Sitecom5FAB74", and "Authentication Mode : WPA2 pre-shared key". A "Passphrase Key" field contains the text "FKL9BMCPLZ83". At the bottom, there are two sections: "WPS Via Push Button" with a "Start to Process" button, and "WPS Via PIN" with an empty input field and a "Start to Process" button.

WPS Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.

Self Pin Code This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID This is the network broadcast name (SSID) of the router.

Authentication Mode It shows the active authentication mode for the wireless connection.

Passphrase Key It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

WPS via Push Button Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

12 Firewall Settings

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select **Enable** and click **Apply**.

The screenshot shows the configuration interface for a Sitecom wireless mobile router 300N. The top navigation bar includes links for Status, Wizard, Wireless Settings, Firewall (which is highlighted), Advanced Settings, and Toolbox. A language selection dropdown is also present. Below the navigation bar, there are tabs for Firewall settings: Enable, DMZ, DoS, Access, and URL block. The 'Enable' tab is selected. The main content area contains a descriptive paragraph about the router's firewall protection and a section for enabling or disabling the firewall module function. The 'Enable' radio button is selected. An 'Apply' button is located at the bottom right of the form.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings **Firewall** Advanced Settings Toolbox Choose your language ▼

Enable DMZ DoS Access URL block

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of a hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Enable or disable Firewall module function : ☒ Enable ☐ Disable

Apply

DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings **Firewall** Advanced Settings Toolbox Choose your language

Enable **DMZ** DoS Access URL block

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

☒ **Enable DMZ**

Public IP Address	Client PC IP Address
<input checked="" type="radio"/> Dynamic IP Session 1 <input type="radio"/> Static IP	<input type="text"/>

Add Reset

DMZ table:

NO.	Public IP Address	Client PC IP Address	Select
1	---	192.168.0.100	<input type="checkbox"/>

Delete Selected Delete All Reset

Apply Cancel

Enable DMZ Enable/disable DMZ

Public IP Address The IP address of the WAN port or any other Public IP addresses given to you by your ISP

Client PC IP Address Fill-in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.



Ping of Death Protections from Ping of Death attack

Discard Ping From WAN The router's WAN port will not respond to any Ping requests

Port Scan Protects the router from Port Scans.

Sync Flood Protects the router from Sync Flood attack.

Access

You can restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.). Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings **Firewall** Advanced Settings Toolbox Choose your language ▼

Enable DMZ DoS **Access** URL block

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC uses what services or has access to.
If both MAC filtering and IP filtering are enabled, the MAC filtering table will be checked first.

☐ Enable MAC filtering ☒ Deny ☐ Allow

Client PC MAC Address	Comment
<input type="text"/>	<input type="text"/>

MAC Filtering table:

NO.	Client PC MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

☐ Enable IP Filtering Table ☒ Deny ☐ Allow

NO.	PC Description	PC IP Address	Client Service	Protocol	Port range	Select
<input type="button" value="Add"/> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>						

Deny If you select "Deny" then all clients will be allowed to access Internet accept for the clients in the list below.

Allow If you select "Allow" then all clients will be denied to access Internet accept for the PCs in the list below.

Filter client PCs by IP Fill in "IP Filtering Table" to filter PC clients by IP.

Add PC You can click Add PC to add an access control rule for users by IP addresses.

Remove PC If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button.

Filter client PC by MAC Check "Enable MAC Filtering" to enable MAC Filtering.

Add PC Fill in "Client PC MAC Address" and "Comment" of the PC that is allowed to access the Internet, and then click "Add". If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.

Remove PC If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

Click <**Apply**> at the bottom of the screen to save the above configuration.

URL block

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The top navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. The 'Firewall' tab is selected, and within it, the 'URL block' sub-tab is active. The interface explains that users can block access to certain web sites by entering a full URL or a keyword. There is a checkbox for 'Enable URL Blocking' which is currently unchecked. Below it is a text input field labeled 'URL/keyword :'. To the left of this field are 'Add' and 'Reset' buttons. Below the input field is a table titled 'Current URL Blocking Table:'. The table has three columns: 'NO.', 'URL/keyword', and 'Select'. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Reset'. At the bottom right of the interface are 'Apply' and 'Cancel' buttons.

wireless mobile
router
300N

STATUS WIZARD WIRELESS SETTINGS **FIREWALL** ADVANCED SETTINGS TOOLBOX Choose your language ▼

Enable DMZ DoS Access **URL block**

You can block access to certain Web sites for a particular PC by entering either a full URL address or just a keyword of the Web site

☐ **Enable URL Blocking**

URL/keyword :

Add Reset

Current URL Blocking Table:

NO.	URL/keyword	Select
-----	-------------	--------

Delete Selected Delete All Reset

Apply Cancel

Enable URL Blocking Enable/disable URL Blocking.

Add URL Keyword Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block.

Remove URL Keyword If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keywords from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

Click <**Apply**> at the bottom of the screen to save the above configurations.

13 Advanced Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.

Port Forwarding

Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.



Enable Port Forwarding Enable Port Forwarding

Private IP This is the private IP of the server behind the NAT firewall.

Type This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only, or select "both" to forward both "TCP" and "UDP" packets.

Port Range The range of ports to be forward to the private IP.

Comment description of this setting.

Add Port Forwarding Fill in the "Private IP", "Type", "Port Range" and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below.

Remove Port Forwarding If you want to remove a Port Forwarding setting from the "Current Port Forwarding Table", select the Port Forwarding setting that you want to remove in the table and then click "Delete Selected". If you want to remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number.

The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The top navigation bar includes tabs for Status, Wizard, Wireless Settings, Firewall, Advanced Settings (selected), and Toolbox. A language selection dropdown is on the right. Below the navigation bar, there are sub-tabs: NAT Enable, Port forwarding (selected), Virtual Server, Special Applications, Application Layer Gateway, uPnP, and Quality of Service. The main content area has a heading "Virtual Server" and a description: "Entries in this table allow you to automatically redirect common network services to a specific PC behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the local network." There is a checkbox for "Enable Port Forwarding". Below it is a form with fields for "Local IP", "Type" (a dropdown menu set to "Both"), "Port range" (two input fields separated by a hyphen), and "Comment". There are "Add" and "Reset" buttons. Below this is a section titled "Current Port Forwarding Table:" which contains a table with columns: NO., Local IP, Type, Port range, Comment, and Select. Below the table are buttons for "Delete Selected", "Delete All", and "Reset". At the bottom right are "Apply" and "Cancel" buttons.

Local IP	Type	Port range	Comment
<input type="text"/>	Both	<input type="text"/> - <input type="text"/>	<input type="text"/>

Buttons: Add, Reset

Current Port Forwarding Table:

NO.	Local IP	Type	Port range	Comment	Select
-----	----------	------	------------	---------	--------

Buttons: Delete Selected, Delete All, Reset

Buttons: Apply, Cancel

Enable Virtual Server Enable Virtual Server.

Private IP This is the LAN client/host IP address that the Public Port number packet will be sent to.

Private Port This is the port number (of the above Private IP host) that the below **Public Port** number will be changed to when the packet enters your **LAN** (to the LAN Server/Client IP).

Type Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "both" setting. **Public Port** Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN.

Comment The description of this setting.

Add Virtual Server Fill in the "Private IP", "Private Port", "Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below.

Remove Virtual Server If you want to remove Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want to remove all Virtual Server settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Special Applications

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings Firewall **Advanced Settings** Toolbox Choose your language ▼

NAT Enable Port forwarding **Virtual Server** Special Applications Application Layer Gateway uPnP Quality of Service

You can configure the router as a Virtual Server allowing remote users to access services such as Web or FTP at your local PC. Depending on the requested service (TCP/UDP) port number, the router will redirect the external service request to the appropriate internal server (located at one of your local PCs).

☐ Enable Virtual Server

Local IP	Local Port	Type	Public Port	Comment
<input type="text"/>	<input type="text"/>	Both ▼	<input type="text"/>	<input type="text"/>

Current Virtual Server Table:

NO.	Local IP	Local Port	Type	Public Port	Comment	Select
-----	----------	------------	------	-------------	---------	--------

Enable Trigger Port Enable the Special Application function.

Trigger Port This is the out going (Outbound) range of port numbers for this particular application.

Trigger Type Select whether the outbound port protocol is "TCP", "UDP" or both.

Public Port Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624).

Public Type Select the Inbound port protocol type: "TCP", "UDP" or both

Comment The description of this setting.

Popular applications This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the

Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

Add Special Application Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". The Special Application setting will be added into the "Current Trigger-Port Table" below. If you happen to make a mistake, just click "Clear" and the fields will be cleared.

Remove If you want to remove Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

ALG

You can select applications that need "Application Layer Gateway" support.

The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The top navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings (selected), and Toolbox. A language selection dropdown is on the right. Below the navigation bar, a sub-menu contains links for NAT Enable, Port forwarding, Virtual Server, Special Applications (selected), Application Layer Gateway, uPnP, and Quality of Service.

Below the sub-menu, there is a descriptive text block: "Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the 'Trigger Port' field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic."

Below the text, there is a checkbox labeled "Enable Trigger Port". Below this, there is a table with the following columns: Trigger port, Trigger type, Public Port, Public type, and Comment. The table is currently empty.

Below the table, there is a section labeled "Popular applications:" with a dropdown menu "Select an application" and an "Add" button. Below this, there are "Add" and "Reset" buttons.

Below the buttons, there is a section labeled "Current Trigger-Port Table:" with a table with the following columns: NO., Trigger port, Trigger type, Public Port, Public type, Comment, and Select. The table is currently empty.

Below the table, there are buttons for "Delete Selected", "Delete All", and "Reset". At the bottom right, there are "Apply" and "Cancel" buttons.

Enable select enable "Application Layer Gateway", then the router will let the selected application correctly pass through the NAT gateway.

UPnP

With UPnP, all PCs in your Intranet will discover this router automatically, so you don't have to configure your PC and it can easily access the Internet through this router.



UPnP Feature You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP and Vista, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

QoS

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference ...etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

wireless mobile
router
300N

SITECOM

Status Wizard Wireless Settings Firewall **Advanced Settings** Toolbox Choose your language ▼

NAT Enable Port forwarding Virtual Server Special Applications Application Layer Gateway uPnP **Quality of Service**

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

☐ Enable QoS

Current QoS Table :

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select
----------	-----------	------------------	--------------------	--------

Enable/Disable QoS You can check "Enable QoS" to enable QoS functionality for the WAN port.

Add a QoS rule into the table Click "Add" then enter a form of the QoS rule. Click "Apply" after filling out the form the rule will be added into the table.

Remove QoS rules from the table If you want to remove QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete".

Selected". If you want remove all QoS rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Edit a QoS rule Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "**Apply**" after editing the form and the rule will be saved.

Adjust QoS rule priority You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

14 TOOLBOX Settings

Password change options

You can change the password required to log into the broadband router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.



The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The top navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. Below this, a sub-menu shows Password, Timezone, Remote, Firmware, Back-up, Reset, and DDNS. The Password section is active, displaying instructions: "You can change the password which is required to log on to the router. By default, the password is admin. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive." Below the instructions are three input fields labeled "Current Password :", "New Password :", and "Confirm Password :". At the bottom right of the form are "Apply" and "Cancel" buttons.

Current Password Fill in the current password to allow changing to a new password.


New Password Enter your new password.

Confirmed Password Enter your new password again for verification purposes.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.



The screenshot shows the configuration interface for a Sitecom wireless mobile router 300N. The page title is "wireless mobile router 300N" with the Sitecom logo. A navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is labeled "Choose your language". Below this is a sub-navigation bar with tabs for Password, Timezone (selected), Remote, Firmware, Back-up, Reset, and DDNS. The main content area is titled "Set the time zone of the Broadband router. This information is used for log entries and firewall settings." It contains three configuration sections: "Set Time Zone" with a dropdown menu showing "(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London"; "Time Server Address" with a text input field containing "europe.pool.ntp.org"; and "Daylight Saving" with an "Enable" checkbox and date pickers for "From" and "To" (both set to January 1). "Apply" and "Cancel" buttons are at the bottom right.

Set Time Zone Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address You can set an NTP server address.

Enable Daylight Savings The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).

Start Daylight Savings Time Select the period in which you wish to start daylight Savings Time.

End Daylight Savings Time Select the period in which you wish to end daylight Savings Time.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.



The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The top navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. Below this, a sub-menu contains Password, Timezone, Remote, Firmware, Back-up, Reset, and DDNS. The 'Remote' tab is selected. The main content area contains a text box explaining the remote management function: 'The remote management function allows you to designate a host from the Internet to have management/configuration access to the router from a remote site. Enter the designated host IP Address in the Host IP Address field.' Below this text is a table with three columns: Host Address, Port, and Enable. The Host Address column has an empty text input field. The Port column has a text input field containing '8080'. The Enable column has a checkbox that is currently unchecked. At the bottom right of the table are 'Apply' and 'Cancel' buttons.

Host Address	Port	Enable
<input type="text"/>	<input type="text" value="8080"/>	<input type="checkbox"/>

Apply Cancel

Host Address This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

Port The port number of the remote management web interface.

Enabled Select "**Enabled**" to enable the remote management function.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Firmware Upgrade

This page allows you to upgrade the router's firmware.



The screenshot shows the web interface of a Sitecom wireless mobile router 300N. The top header includes the text "wireless mobile router 300N" and the "SITECOM" logo. Below this is a navigation bar with tabs: "Status", "Wizard", "Wireless Settings", "Firewall", "Advanced Settings", and "Toolbox". A "Choose your language" dropdown menu is located on the right. Under the "Toolbox" tab, there is a sub-menu with "Password", "Timezone", "Remote", "Firmware", "Back-up", "Reset", and "DDNS". The "Firmware" tab is selected. The main content area contains the following text: "This tool allows you to upgrade the Routers firmware. Browse to and select the upgrade file and click APPLY. You will be prompted to confirm the upgrade." Below this text is a text input field followed by a "Browse..." button. At the bottom right of the form are "Apply" and "Cancel" buttons.

Firmware Upgrade This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process.

Backup Settings

The Backup screen allows you to save (Backup) the router's current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).



The screenshot shows the configuration interface for a Sitecom wireless mobile router 300N. The top navigation bar includes links for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. Below this, a secondary bar contains links for Password, Timezone, Remote, Firmware, Back-up, Reset, and DDNS. The main content area is titled "Back-up" and contains the following text: "Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings." Below this text are three rows of controls: "Restore To Factory Default" with a "Reset" button, "Backup Settings" with a "Save" button, and "Restore Settings" with a text input field, a "Browse..." button, and an "Upload" button.

Use the "Backup" tool to save the Broadband router current configuration to a file named "**config.bin**" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system.



Click <**Apply**> at the bottom of the screen to save the above configurations.

DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

The screenshot shows the DDNS configuration page of a Sitecom wireless mobile router 300N. The page has a header with the router model and a navigation bar with tabs: Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. Below the navigation bar is a sub-menu with tabs: Password, Timezone, Remote, Firmware, Back-up, Reset, and DDNS. The DDNS tab is selected. The main content area contains a description of DDNS and a form with the following fields: Dynamic DNS (radio buttons for Enable and Disable, with Disable selected), Provider (a dropdown menu showing 3322(qdns)), Domain Name (a text input field), Account/E-mail (a text input field), and Password/Key (a text input field). At the bottom right of the form are Apply and Cancel buttons.

Enable/Disable Enable or disable the DDNS function of this router.

Provider Select a DDNS service provider.

Domain name Fill in your static domain name that uses DDNS.

Account/E-mail The account that your DDNS service provider assigned to you.

Password/Key The password you set for the DDNS service account above.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Parts of the firmware of the WLR-2002 Wireless Mobile router are subject to the [GNU general public license](#).

Appendix A: Licensing Information

This product includes third-party software licensed under the terms of the [GNU General Public License](#). You can modify or redistribute this free software under the terms of the [GNU General Public License](#). Please see Appendix B for the exact terms and conditions of this license.

Specifically, the following part of this product is subject to the GNU GPL:

#	Package name	Source
1	Linux v2.6.21	www.kernel.org
2	Iptables v1.3.5	www.netfilter.org/
3	Bridge-utils v1.2	bridge.sourceforge.net/
4	Busybox v1.7.5	www.busybox.net/
5	Rp-pppoe v3.8	freshmeat.net/projects/rp-pppoe/
6	Pptp-client v1.7.1	pptpclient.sourceforge.net/
7	Ppp v2.4.3	ppp.samba.org/
8	Udhcp v0.9.9-pre	udhcp.busybox.net/
9	iproute2 v2.6.16-060323	www.linux-foundation.org/en/Net:Iproute2
10	Dnsmasq v2.39	www.thekelleys.org.uk/dnsmasq/doc.html
11	Ez-ipupdate v3.0.11b8	ez-ipupdate.com/
12	Libupnp v1.6.0	upnp.sourceforge.net/
13	Wireless-tools v28	RaLink SDK 3.1.0.0
14	U-boot v1.1.3	RaLink SDK 3.1.0.0
15	gcc-3.3.6	RaLink SDK 3.1.0.0
16	Uclibc-0.9.29	RaLink SDK 3.1.0.0

Availability of source code

Sitecom Europe BV has made available the full source code of the GPL licensed software, including any scripts to control the compilation and installation of the object code in the driver section of this product on the Sitecom website.

No Warranty

The free software included in this product is distributed in the hope that it will be useful, but WITHOUT ANY LIABILITY OF OR ANY WARRANTY FROM THE LICENSOR.

Appendix B: GNU GENERAL PUBLIC LICENSE

Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if

you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights. We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0.

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2.

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other

licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3.

You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4.

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free

software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10.

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11.

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS